State of Vermont

Change Control Policy

Date: 11-02-10
Approved by: Tom Pelham
Policy Number:

Table of Contents

1.0 Introduction

1.1 Authority

The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), "to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government."

Managers, employees, records personnel, third party vendors and all others who connect to or handle State of Vermont networks and data are responsible for reviewing this policy in concert with business, legal, and information technology staff to ensure that the policy (1) meets legal requirements specific to the agency and its data and (2) can be effectively carried out by agency employees. If laws or regulations require more stringent requirements than stated in this policy, the internal policy created by the agency must explicitly state the more stringent requirements. Agencies shall not develop an internal policy with requirements lower than the minimum requirements listed in this policy.

1.2 Purpose

The purpose of this policy is to establish a statewide approach to technical change control. Information technology (IT) and business teams must manage system changes in a rational and predictable manner. Changes require planning, monitoring, testing and follow-up evaluation to reduce negative impact to the user community and to increase the value of information resources. This policy is not intended to be a statement of the current technical change control practices of state agencies. It is a statement of goals and expectations. Meeting these goals and expectations are necessary to insure well managed evolution of information technology systems.

1.3 Scope

For the purpose of this policy, department refers to any State entity including agencies, departments, boards and councils or other entities in the executive branch of government.

The following non-exhaustive list depicts common types or reasons for system changes:

- User requests
- Vendor recommended/required changes
- Changes in regulations
- Hardware and/or software upgrades
- Acquisition/implementation of new hardware or software
- Hardware or software failures
- Changes or modifications to the infrastructure
- Environmental changes (electrical, air conditioning, data center remodels, etc)

- Unforeseen events
- Periodic Maintenance
- Application modifications and enhancements
- Patch deployment

2.0 Policy

Information technology systems are subject to formal change control processes. Such processes provide a managed and orderly method by which changes are requested, tested, approved, communicated prior to implementation (if possible), and logged. Attributes of a formal change control process/procedure include:

- Assignment of a technical change manager or change control team
- Written change requests submitted for all changes, both scheduled and unscheduled.
- Change requests receive formal approval before proceeding with the change.
- A testing plan is required to include IT and business representatives where appropriate.
- Customer notification is completed for each scheduled or unscheduled change
- A post change review is completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A change log is maintained for all changes. The log should contain, but is not limited to:
  - Date of submission and date of change
  - Owner and custodian contact information
  - Nature of the change
  - Indication of success or failure

Change control procedures for patches may require resources and processes very different from application change control, where for example a formal change control board may be required. Departments should develop procedures and documentation that are appropriate to the change, level of risk, organizational structure and audit requirements.

The following is a list of user roles and the responsibilities associated with those roles:

1. End-User/Functional User
   i. Submitting change requests
   ii. Participating in user testing, pre-deployment testing and post deployment testing
   iii. Sign off on the change where appropriate
   iv. End/Functional User Management
   v. Verifying that change requests are valid
   vi. Sign off on changes where appropriate
2. IT Staff are sometimes end users, functional users, or functional user managers, and as such have responsibility for following this policy.
3. IT Staff Technician Role – follows a prescribed change control process/procedure.

4. IT Management – overall responsibility for overseeing change control policy and processes, e.g. policy dissemination, oversight, and implementation approval of changes.

3.0 Policy Notification

Each state agency is responsible for ensuring that employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.